Draft ISMG Meeting Minutes

Date: January 26, 2012
Time: 1:00 pm
Location: Mitchell building, room 218

Attendees

Rick Bush, TRS; Dan Delano, DOJ; Cleo Anderson, DOR; Kristi Antosh, MDT; Kimberly McIntyre, COR; Michael Sweeney, DOA; Dawn Harmon, SAO; Sarah Bagg, FWP; Jim Ashmore, SITSD; Chris Silvonen, DPHHS; Jackie Thiel, DPHHS; Bill Anker, DNRC; Terry Meagher, DOC; and Jaclyn Hardamon, SITSD.

Call to Order – Jim Ashmore

- Jim called the January meeting to order.

Approval of Minutes – ISMG

- Jim asked for comments or changes to the December minutes.
  **** Action Item****
- Rick offered a motion to approve the minutes. Kim seconded.
  - Motion passed unanimously.
- Jim reminded everyone of the shared documents site for their use and reference at SharePoint site.

ISM Risk Strategy Guide_1240.G02 – ISMG

**** Action Item****

- Rick asked what the significance was in the numbering on the front page. Jim clarified that the 1240 number is the group structure, the G stands for Guide and 02 is a sequential number. The number 01 is reserved for the index that Jim is working on putting together once the Guide is completed. Jim also mentioned that the numbering system will probably be going away and just use titles instead.
- Jim asked the group if a subsection is needed for the Trust and Trustworthiness section. The group said to leave it in as it is a guide and the different groups will use what they need from it. Kristi corrected some spelling errors.
- Michael recommended getting the guide out instead of reviewing it section by section as it will be a living document and updates can always be made.
- Dan had a few changes and wanted to move a few things around. He would also like to not have the "hearing" section as its own category. Kristi Antosh likes it as its own section so people can see the differences in the sections. Dan clarified that he just would like the word "hearing" to be different. Sarah mentioned possibly putting it above "written" and putting it with "eavesdropping". The group identified a few misspellings. Jim also explained the approval process.
- Dan offered a motion to approve the guide. Michael seconded.
  - Motion passed unanimously.

DPHHS Risk Management Program – Jackie Thiel

- Roles and responsibilities:
  - 5 basic types of people
    - Senior Management
    - Computer Security Management
    - System Administrators
    - Users of the information
    - Operational Support Personnel
  - Matrix (pg 13) for IT Security Roles and what those roles are responsible for.

    - Attachment "A" will be updated whenever necessary since that is the actual names and list of groups of people.
    - Kristi asked if this was all done before 2009. Jackie said yes, all of this was done before 2009.
- Security awareness and training:
    - Jackie said they do most of their training in October.
    - Discussed SANS and that they will be buying 1,000 seats this year.
- Planning:
    - Their documents are confidential.
    - Jackie said they have done an Enterprise security plan.
    - Jim asked if they are part of the strategic plan. Jackie said they are separate.
    - Jackie said they have 5 of 6 plans done and most have a risk assessment as well.
- Risk Assessment:
    - Management Summary Report gives details that are given to the data owner and then it is up to them to decide to determine whether or not it is cost efficient to implement the controls or accept the risk.
    - Executive Summary Report shows deficiencies and vulnerabilities, such as better training for everyone.
    - Jim asked about the action plan. Jackie said they move data to the next level of the data owner and also discussed their theory.
    - Risk Assessment Characterization and Prioritization Tool
        - Characteristics of Programs (scoring). The business owners mostly fill it out themselves or ask for help on the questions they don't know.
        - Risk Management
        - People
        - Policy and Processes
    - The staff doesn't get the last (scoring) page. When the risk score is high a FRAAP is conducted, Moderate risk score requires the Risk Assessment checklist, and a low assessment requires no further risk assessment activity.
    - Checklist (Full, partial or no compliance), system owners filled this out.
    - FRAAP Procedure is not shared with the staff.
    - FRAAP Threat Checklist (Excel spreadsheet)
    - Controls are put into place. Mostly the system owners fill this out but the tech personnel will also help.
    - Write the report
    -
- Authorization and Certification Process:
    - This area is one that DPHHS has not yet implemented. Will work on this in 2012

- Jim asked Jackie how she updates their plan. She discussed their plan and how it is detailed.
- The group discussed procedures, testing and security policy procedures.
- Kristi asked if they have a template. Chris said he has one but sometimes it is not helpful without all the information which cannot be shared outside of DPHHS. Kristi volunteered Jim to go to DPHHS to look at their plan and with Chris and Jackie's help, to create a template for everyone to use.
- Kristi offered a motion for Jim to create a template after reviewing Jackie's plan. Everyone agreed.
    - Motion passed unanimously. Jim said he would be glad to help.
- Jackie and Chris discussed the importance of having a Security plan from the beginning and setting up a plan.

Device Sanitation & Disposal Guide_1240.G03 – ISMG

- It is not a policy it is a tool to be used to give focus and assistance in managing the life cycle of information security assets.
- The Full Life Cycle needs to be defined in our programs.
- Jim said it might replace the current policy. He said they are looking in to it.
- Jim asked for everyone to e-mail him questions before the next meeting.

SANS Update-Purchase New seats open Jan 15 – Feb 29, 2012 – Jim

- The purchase of SANS is open now through the 29th of February.
- The license is good for 12 months; however Jim will verify and confirm.
- The group thought the expiration date is June or July. Jim said he will verify and confirm.
- The SANS don't get assigned to a person until you assign them.
- Kristi talked about a list Lynne Pizzini had that showed what the modules are and the amount.
- Jim said there are also reporting abilities as well.

(NEW) Contract/RFP Language – Jim

- Jim will be meeting with the SITSD procurement division to get their perspective, help and interaction on contract structure and the process as well as the language.
- Kristi asked about the CEP and if Jim could include it as well as it would be helpful.
- Rick also mentioned adding an addendum.
- Jim said he would have a draft by the next meeting.

(NEW) Training & Awareness – Jim/ISMG

- Jim would like to take 15 minutes for training in the monthly meetings. The group discussed who would set-up the trainings, such as professionals or even group round tables. Rick thought next month could be device sanitation and disposal. Dan discussed their laptops and how to sanitize them.
- Jim mentioned NIST and other certification agencies.
- Jackie brought up Lynne discussing NIST.
- Kristi discussed training for everyone for possibly a half day training.
- Rick discussed ISMG and securing servers as training to be helpful for the group.
- Cleo wanted to know if the extended training would be open to more people than just this group as she said she has a task force and it would be beneficial to them to attend as well. Jim said he will open it up to everyone to attend.
- Sarah asked if there is a fee for Jim to come into the departments and help. Jim clarified that there is no additional fee.
- Jim asked for thoughts from the group and he will look into how to help each program. He said to please e-mail him.
- Jackie asked the group for a running list of training as well. Jim will talk to Miranda Keaster about a list. He also said she is working on the training site as well as a training catalog.
- Dawn mentioned some training and will forward the information to Jim.
    - Provided by Dawn Harmon - http://www.teex.org/teex.cfm?pageid=agency&area=OGT&templateid=1810
    - Provided by Dan Delano - http://iase.disa.mil/eta/

Discussion - Policy vs. Plan; what is compliance? – Jim/ISMG

- Jim said he met with Dick Clark, Tammy LaVigne and Stuart Fuller; they are working through it and he will let everyone know as soon as possible or at the next meeting.
- Jim said he would like a clear definition on whether it is a policy, a plan or something else that constitutes "compliance", also if the deadline is flexible.

(TABLED) Review of ISM Program Policy Doc (optional use) – ISMG

- Still available for review and will readdress after clarification from CIO office for policy requirement.

2012 Agenda Focus – All

- Jim asked the group to e-mail him ideas and focuses for the next year.
- Rick recommended an Open House Workshop for what is needed for July 1, 2012 but Jackie said it depends on what the CIO and director of DOA decides regarding the Policy Program Plan.
- Kristi discussed a Strategy Guide.
- The group discussed policies, guides and the law for each agency.
- Jackie discussed the SISTD policy that requires that agencies to have a security program aligned with FISMA and NIST 800.39 and 800.53.
- Jim said he will get the information to everyone as soon as possible and hopefully will be able to put together a training session for February.
- Jackie said if they have to do a policy that it would take their legal and all of the approval processes a while as it is currently taking over 18 months for an e-mail and an internet policy. She said they wouldn't be ready by July 1st.
- Jim asked the group if there was an Enterprise policy would their agency directors accept it? Jim said NIST is interpreted many different ways. The group discussed a new policy and possibly extending the timeline. The group also discussed Plan vs. Policy. Jim drafted a document for Dick Clark to consider.

Other Business? – All

- February 23rd, 2012 is the next scheduled meeting.

Adjourn – All

****Action Item****

- All moved to close.
- The vote was unanimous. The meeting adjourned at 2:42pm.